AF-TRUST

Air Force Team for Research in Ubiquitous Secure Technology

AF-TRUST

Air Force Team for Research in Ubiquitous Secure Technology

Final Performance Report

July 26, 2010

Principal Investigator: S. Shankar Sastry
Lead Institution: University of California, Berkeley
Address: Regents of the University of California
The University of California, Berkeley
2150 Shattuck Avenue, Room 313
Berkeley, California 94720-5940

AF-TRUST is funded by the Air Force Office of Scientific Research (agreement number FA9550-06-1-0244)

Berkeley UNIVERSITY OF CALIFORNIA Cornell University  VANDERBILT UNIVERSITY

TABLE OF CONTENTS

1 PROGRAM OBJECTIVES

The Air Force Team for Research in Ubiquitous Secure Technology (AF-TRUST) was established as a U.S. Air Force Partnership for Research Excellence and Transition (PRET) center for research on challenges associated with the Global Information Grid (GIG) and Network Centric Enterprise System (NCES) trends that have become dominant themes within the Air Force and the military. The AF-TRUST team was focused on top Air Force research priorities to unify three major enterprise Air Force subsystems and to link the Air Force network with networks operated by other Department of Defense (DoD) Services.

The objective of AF-TRUST was to advance the state-of-the-art in cyber-assurance to address key trust- and Quality of Service (QoS)-related properties simultaneously throughout the lifecycles of large-scale Air Force systems via a novel combination of analytical and experimental techniques. The program focused on innovations in the following three areas:

1. ***Scalable, Real-Time, and Fault-Tolerant Quality of Service (QoS).*** Many Air Force applications, particularly those in the domains of tactical information management and command and control, demand rapid responsiveness, high availability, and individual information services to support huge numbers of clients. However, the GIG/NCES technology base (Web Services) was developed for operators of commercial data centers, where such QoS requirements are relatively uncommon. The AF-TRUST team investigated technical solutions and showed how emerging standards and Commercial-Off-The-Shelf (COTS) technologies can be augmented with these technologies to remedy the gaps.

2. ***Very Large-Scale Information Assurance and Security Policy Management.*** The Air Force increasingly needs to port legacy systems into a "single dark core" network without fear of security or reliability exposures. The AF-TRUST team investigated novel network-level containment options that link virtual private networks, virtual machine monitors, and powerful management tools to automate the administration and tracking of key material, firewall configuration information, and security policies with an emphasis on defining a concrete engineering vision to enable specific security capabilities matched to specific needs arising from the GIG/NCES.

3. ***Scalable and Secure Discovery, Information Architecture, and Mediation.*** The NCES architecture includes a discovery component, consisting of technologies to assist information clients in finding information providers and mediation solutions to help in standardizing the subsequent information exchange. Yet the Web Services standards on which this will be based do not "scale up" for use in large settings. That is, Web Services assumes applications are designed to peer with a known data center; however GIG/NCES technology base must handle vast numbers of clients seeking services within vast pools of providers subject to security policies. The AF-TRUST team investigated new technologies to solve these tough and important problems using Air Force scenarios identified jointly through dialog with the Air Force Research Laboratory (AFRL) and other DoD researchers and developers.

It is our conviction that existing and emerging COTS software and systems will not deliver enterprise management, information management, or discovery tools, nor will they provide real-time, scalable, multi-level security solutions that the DoD and the Air Force will need for its operational and tactical information management systems. This effort worked to address challenges raised by the DoD's unique needs by developing new algorithms, protocols, software platforms, and tools in collaboration with industry partners and the Air Force/DoD customers.

2 PROGRAM OVERVIEW

This work of this program was intended to address important, high-value issues to the Air Force. The proposed activities were shaped by a series of studies in 2005 led by AF-TRUST Principal Investigator (PI) Shankar Sastry from UC Berkeley and AF-TRUST Co-PI and Chief Scientist Prof. Ken Birman from Cornell on behalf of the Air Force Chief Information Officer (CIO) to quantify the challenges of information assurance, security, and survivability of Air Force networks at the enterprise, tactical, embedded systems and command and control levels. From these studies, commissioned by Dr. Sekar Chandersekaran of the Secretary of the Air Force's Warfighting Integration and CIO office (SAF/XCX)), a number of key findings resulted which motivated the work of AF-TRUST. In particular:

1. The GIG and NCES opportunity is transformational, with implications at every level—from the cost of developing enterprise network solutions (efficiencies, productivity improvements, elimination of stovepipe boundaries to enable new integrated applications) to tactical solution for the network embedded systems (new capabilities exploiting integrated legacy data sources), and even doctrinal solutions (better information for strategists and warfighters, permitting unparalleled flexibility and smarter combat activities).

2. Issues for addressing information assurance and survivability abound at all levels, including the enterprise level, command and control level, and the tactical level.

3. Realization of these ambitious opportunities requires that technology gaps be identified and filled. The COTS technology base on which GIG and NCES will be constructed (e.g., Windows/.NET, Web Services, Linux and CORBA) are powerful starting points but leave profound questions unanswered.

The AF-TRUST program was supported by teams of researchers at Cornell University, Vanderbilt University, and the University of California, Berkeley. Below are brief summaries of each university team's focus and contribution:

- The Cornell team developed software systems responsive to Air Force articulated needs (e.g., the Live Objects platform and Ricochet time-critical eventing protocol) and ran the AFOSR-sponsored workshop on risks of homogeneous system deployments. Briefings were done at many levels, including AFOSR and the AF/CIO and AF/XC. Software deliverables have been picked up by a number of organizations, including AFRL.

- The Vanderbilt team worked on aspects of model-based security, including methods and tools for expressing security concepts using domain abstractions and translating them into underlying mechanisms, protocols, and implementation. This focused developing models and implementations of attack agents, specifically Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks and testing the components by simulating the Leader-Follower control for a UAV group and demonstrating how DDoS attacks destabilize the formation.

- The UC Berkeley team developed techniques to assure high security for platforms like the GIG. They developed a framework for ensuring that information input into the GIG has high integrity via a trusted path from remote sensing terminals (including wireless) encompassing the embedded system, communications, and information presentation. They also developed techniques for increasing user assurance of information to provide it in a fashion that users can use and trust.

3 PROGRAM ACTIVITIES

The following sections describe in more detail the key research and development activities in each of the three areas described in Section 1.

3.1 Scalable, Real-Time, and Fault-Tolerant Quality of Service (QoS)

Many Air Force applications require predictably fast performance, even in the face of many active clients. We have developed Live Distributed Objects (LDO), a new programming model and a platform, in which instances of distributed protocols are modeled as components with an object-oriented look and feel that can be composed in a type-safe manner to build complex distributed applications using a simple, intuitive drag and drop interface. To support this and other distributed systems platforms, we have developed a collection of techniques: approach to modeling the semantics of distributed multi-party protocols such as leader election, distributed locking, or reliable multicast, and a programming language that supports it. Specifically, we developed a new object-oriented approach to modeling the semantics of distributed multi-party protocols such as leader election, distributed locking, or reliable multicast, and a programming language that supports it. We introduced a *distributed flow*, a stream of messages flowing concurrently at multiple locations. Our flows correspond to variables and method parameters in Java-like languages. Active protocol instances consume and output flows; their internal states are encapsulated as internal flows, and all of their internal logic is represented as operations on flows. Our language supports a new type of concern separation: the semantic structure of protocols is decoupled from implementation details such as the construction and maintenance of overlays, trees, or other hierarchical structures needed for scalability.

We developed various novel ultra-reliable multicast and multi-destination data streaming protocols. We list here a few of these:

- *Ricochet*, a low-latency reliable multicast protocol designed for time-critical clustered applications. It uses IP Multicast to transmit data and recovers from packet loss in end-hosts using Lateral Error Correction (LEC), a novel repair mechanism in which XORs are exchanged between receivers and combined across overlapping groups. Data centers avoid IP Multicast because of a series of problems with the technology.
- *Dr. Multicast* (the MCMD), a system that maps traditional IPMC operations to either use a new point-to-point UDP multisend operation, or to a traditional IPMC address. The MCMD is designed to optimize resource allocations, while simultaneously respecting an administrator-specified acceptable-use policy.
- *QuickSilver*, a platform for reliable multicast in very large environments. The current version of QuickSilver features QuickSilver Scalable Multicast (QSM), a new multicast protocol with probabilistic guarantees, optimized for high throughput. QSM achieves throughputs close to the network limits with very low CPU overhead, and exhibits almost no performance degradation when scaled to 200 nodes and 8000 groups.

Additional work focused on the foundations of software component technologies that directly reflect concurrency, timeliness, and fault tolerance. Whereas today's software components are objects (mostly passive components, that interact via procedure calls), tomorrow's software components must be actors (active, concurrent components that interact via messaging). The key outcome was to develop design techniques that support safely composable real-time subsystems. The focus was on interface specifications for components that include timing information so as to ensure that timing properties of one component do not disrupt required timing behavior of another.

Additional work investigated techniques for effectively managing multiple resources, such as processing power and network bandwidth, simultaneously in distributed real-time and embedded (DRE) systems that execute in open environments. To address this research question, we designed and developed the Hierarchical Distributed Resource-management Architecture (HiDRA), which provides adaptive resource management using control techniques that adapt to workload fluctuations and resource availability. In contrast to adaptive control techniques that manage only one type of system resource, HiDRA features a hierarchical control scheme that manages both bandwidth and processor utilization simultaneously.

This work also investigated techniques for decoupling adaptive resource management algorithms from the underlying middleware implementation, thereby enabling the usage of various resource management algorithms without the need for redeveloping significant portions of the middleware. To address this research question, we developed the Resource Allocation and Control Engine (RACE), a fully customizable and configurable adaptive resource management framework for DRE systems. RACE can be configured to support a range of algorithms for adaptive resource management without requiring modifications to the underlying middleware. To enabling the seamless integration of resource allocation and control algorithms into DRE systems, RACE enables the deployment and configuration of feedback control loops, thereby complementing theoretical research on adaptive resource management algorithms that provide a model and theoretical analysis of system performance.

This work also investigated techniques to effectively decouple crosscutting deployment and configuration (D&C) concerns (e.g., real-time QoS concerns and middleware service configuration concerns) from different layers of core component middleware infrastructure, ranging from components, containers, and component servers. To address this research question, we developed a middleware framework that uses aspect-oriented techniques to selectively customize and configure different middleware features. The novelty of this technique stems from the aspect-oriented techniques it uses to decouple D&C concerns, such as configuring server resources and real-time policies for software components, resulting in a highly optimized configuration framework the supports much better component reusability and extensibility than conventional approaches.

This work also investigated techniques to meet the scalability requirement and real-time QoS requirements for large-scale deployment and configuration. To address this research question, we developed a high-performance distributed middleware D&C toolchain called the Deployment And Configuration Engine (DAnCE). The novelty of DAnCE is its ability to enhance system performance by allowing QoS specifications and enforcement mechanisms to change both at design-time and run-time based on the target deployment environment and application requirements. DAnCE provides a set of highly optimized D&C platform and reusable infrastructure for component-based DRE systems.

Finally, additional work addressed the challenges associated with security of control systems and cyber-physical systems. Control systems, computer-based systems that monitor and control physical processes, and cyber-physical systems, systems that integrate computing and communications with monitoring and control of physical entities, both serve mission-critical roles in military and civilian applications. While most of the effort for protecting CPS has been done in reliability (the protection against random failures), there is a growing concern for the protection against malicious cyber attacks. This is due, in part, to advances in control systems technologies and implementations. For example, original control devices that were designed as electromechanical relays are being replaced by devices that contain microprocessors and embedded operating systems. Often times these devices are networked, employ COTS solutions, and leverage open communications protocols—all of which make control systems more vulnerable. We have investigated various types of attacks against control systems, including *deception attacks* (where the adversary sends false information from sensors and controllers to the system) and

Denial of Service (DoS) attacks (where the adversary prevents a controller from receiving sensor measurements).

3.2 Very Large-Scale Information Assurance and Security Policy Management

Machine learning is becoming prevalent in the systems domain as a detection and analysis tool for problems amenable to adaptive techniques. However, the adaptivity and flexibility that are machine learning's biggest assets are also qualities that an attacker might exploit. Thus, in our research we have studied the security of learning systems. One research direction we have explored experimentally and theoretically is analyzing existing systems, including e-mail spam filtering based on Baysian models and PCA-based network flow anomaly detection in point-to-point flows based on link volume data. We also investigated the effect an adversary can have on the normal subspace of link volume vectors learned under various realistic models of control. In a similar vein, we are exploring the vulnerabilities of the spam filter, SpamBayes.

Additional work focused on the dynamics of interacting adaptive learning algorithms. The research studied the dynamics of repeated interactions between algorithms that each adapt to their past experience to optimize a reward function depending on their own actions as well as those taken by other algorithms participating in the system. A typical motivating example would be the interaction of multiple devices (e.g., cognitive radio nodes) accessing a set of shared congestible resources. Existing work established that if all participating nodes use algorithms from a family known as "no-regret learning algorithms" then the empirical action distribution converges into the set of correlated equilibria of the single-stage game defined by the reward function. Unfortunately the set of correlated equilibria is generally quite large, often leading to multiple widely differing predictions for the outcome of the dynamics. Our research sought to achieve a narrower set of predictions by narrowing the set of algorithms considered to a family of learning algorithms known as "aggregate monotone selection dynamics" or "multiplicative-weights update algorithms", and also to explore the price-of-anarchy implications of this learning-theoretic refinement of correlated equilibrium.

Additional work explored programming language and compiler options for enforcing security policies. The approach leveraged static analysis, in which one looks at code given by a developer, to see whether there are conditions under which the program can be tricked into behaving in an inappropriate or insecure manner. While there has been much work on buffer overflow and return-to-stack attacks, our work looked at much broader questions using program analysis as the lever.

3.3 Scalable and Secure Discovery, Information Architecture, and Mediation

Security protocols, such as key-exchange and key-management protocols, are short, but notoriously difficult to prove correct. Not surprisingly, a great deal of effort has been devoted to proving their correctness. There are two largely disjoint approaches. The first essentially ignores the details of cryptography by assuming perfect cryptography (i.e., nothing encrypted can ever be decrypted without the encryption key) and an adversary that controls the network. By ignoring the cryptography, it is possible to give a more qualitative proof of correctness, using logics designed for reasoning about security protocols. Indeed, this approach has enabled axiomatic proofs of correctness and model checking of protocols. The second approach applies the tools of modern cryptography to proving correctness, using more quantitative arguments. Typically it is shown that, given some security parameter k (where k may be, for example, the length of the key used) an adversary whose running time is polynomial in k has a negligible probability of breaking the security, where "negligible" means "less than any inverse polynomial function of k". There has been recent work on bridging the gap between these two approaches, with the goal of constructing a logic that can allow reasoning about quantitative aspects of

security protocols, while still being amenable to mechanization. We showed how a logic that has already been widely used for nonmonotonic reasoning in Artificial Intelligence (AI) can do just that.

Additional work developed a new way to build secure web applications. Web applications are now an integral part of our infrastructure, yet it is difficult for application developers to ensure that they are meeting security and privacy requirements. In fact, most Internet security vulnerabilities now involve web applications. By contrast, our approach yields security by construction. Programmers write web applications using Jif, a security-typed language that permits information security policies to be expressed explicitly in the program. The compiler can then check that information flows in the web application are secure, and can even extract web application code to run securely on the client browser, as JavaScript. Papers in USENIX Security '07 and SOSP '07 describe this line of work and the software framework we built has been released publicly.

We also studied the problem of building secure voting systems, and constructed a new secure voting system called Civitas. Civitas is a remote voting system that offers strong security guarantees, universal verifiability and coercion resistance, under weaker assumptions than any prior voting system. This is accomplished by using sophisticated cryptographic methods. We implemented Civitas, showing that the system scaled to a large voter base and that the cost of using expensive cryptography was acceptable. The Civitas system is described in our paper in IEEE Security and Privacy '08 and the Civitas tabulation software has been released publicly.

Most recently, we began developing a new infrastructure for building and integrating secure federated systems, called Fabric. Described in our SOSP '09 paper, Fabric is a decentralized system (like Web), but offers a high-level language-based programming abstraction. Distributed and persistent information appears as language-level objects annotated with security policies. This allows easy access to distributed computation and distributed storage, with strong guarantees for information security and consistency. Fabric supports implementation of web servers for easy integration with existing standards. Performance results from Fabric are promising. A Fabric prototype has been implemented and we plan to release the software soon.

4 PROGRAM ACCOMPLISHMENTS/NEW FINDINGS

The sections below describe research highlights in each of the three research areas of the AF-TRUST program described in Section 1.

4.1 Scalable, Real-Time, and Fault-Tolerant Quality of Service (QoS)

A number of applications and tools were developed by the AF-TRUST team, specifically the following:

- The *Live Distributed Objects* platform is available for Windows XP/2003/Vista/2008. The platform has been open-sourced and the source code is hosted at CodePlex (liveobjects.codeplex.com). An initial port to Linux (using the Mono platforms) is available as well. Video demonstrations can be found out http://liveobjects.cs.cornell.edu/.
- The *Quicksilver multicast protocol* (for the Windows/.NET platform) is available for download at http://www.cs.cornell.edu/projects/quicksilver/QSM/. The distribution includes QSM binaries, examples, documentation, and Visual Studio 2005 help files.
- *Ricochet* is a high-speed multicast with extremely low latency. It scales well in numbers of groups. Implementation currently requires Java/Linux and the software can be provided upon request.
- *Dr. Multicast* (MCMD) is compatible with the Posix IP Multicast socket interface. An extension that supports rate limiting (Ajil) is under development and will be made available for distribution. The application code can be provided upon request.
- *Maelstrom* is a completely transparent technology for improving inter-data center connectivity to run on high-speed WAN links despite noise and bursty loss. It runs on Linux and requires one Maelstrom box on each end of the link.
- *Tempest* is a system that provides programmers with data structures that look very similar to conventional Java Collections but are automatically replicated, scaling well in real-world service architectures.
- *Nysiad* is a novel approach to scalable Byzantine fault tolerant protocols and distributed applications written in Erlang. A new, significantly more efficient version is under development and will be made available shortly.
- *Bosco* is the first Byzantine consensus protocol that under favorable circumstances can terminate in one communication round.
- *S-Fireflies* is a self-stabilizing overlay network that is robust against permanent Byzantine faults. The overlay structure has a logarithmic diameter, and can withstand high churn without affecting the ability of correct members to disseminate messages.
- *Firepatch* is a Fireflies-based intrusion-tolerant dissemination mechanism that combines encryption, replication, and sandboxing to prevent hackers from reverse engineering a patch and introduce a virus before the patch is installed.

In addition to the tools listed above, we developed various protocols for estimating data distributions in large peer-to-peer systems, important to the management of such systems.

Additional work provided the seeds for an ongoing effort to develop distributed real-time systems based on model that we call PTIDES, described in the outcome publications. AFRL is using Ptolemy II for building very large scale models of political, social, military, and economic systems in nation building applications.

Our research on HiDRA, RACE, and DAnCE has been integrated into the Component-Oriented ACE ORB (CIAO), www.dre.vanderbilt.edu/CIAO, which is an implementation of the Lightweight CORBA

Component Middleware (CCM) for distributed real-time and embedded (DRE) systems based on the The ACE ORB (TAO), www.dre.vanderbilt.edu/TAO, which is widely use implementation of the Real-time Common Object Request Broker Architecture (CORBA). CIAO and TAO are widely used, open-source DRE middleware frameworks that contain a rich set of components and domain-specific languages that implement patterns and product-line architectures for high-performance DRE systems. These middleware platforms constitute some of the most successful examples of software R&D ever transitioned from research to industry, being widely used by thousands of developers in hundreds of companies including, but not limited to Defense, Aerospace, Finance, Telecommunications, and Internet industries.

In particular, the work on CIAO and TAO middleware for DRE systems has transitioned to the Joint Tactical Terminal (JTT) and Joint Tactical Radio System (JTRS) software defined radio programs, manned/unmanned combat air vehicles, the Orbital Express low earth orbit (LEO) satellite telemetry and control framework, the Ground Support System (GSS) for the X33 Single Stage To Orbit (SSTO) Reusable Launch Vehicle, and the USS Ronald Reagan, the USAF upgraded early warning radar system, the DMSO HLA/RTI and DISA TENA distributed interactive simulation middleware, among many other DoD applications. Likewise, the work on dynamic resource management algorithms and component deployment and configuration middleware for system integration has transitioned to major DoD acquisition programs at Boeing, Lockheed Martin, Northrop Grumman, and Raytheon.

Finally, in the area of secure control systems and secure cyber-physical systems, our work has produced a better understanding of how to secure control systems and cyber physical systems. In particular, we have results that advanced the knowledge of threats, and possible consequences of attacks, on such systems. For example, we have developed an adversary model to help understand the types of attackers, their motivations, and their resources—from disgruntled employees to cybercriminals to terrorists and those acting on behalf of a Nation state. We have also identified the unique properties of control systems and cyber-physical systems to help understand how their securing them differs from securing traditional IT systems. While some traditional IT security techniques can improve the security of control systems and cyber-physical systems, these are not sufficient for providing robust defense-in-depth and there is a need for novel attack-detection and attack-resilient techniques and solutions. Finally, we have investigated security mechanisms for prevention, detection and recovery, and resilience against attacks on control systems and cyber-physical systems. In prevention, much can be gained by the implementation of security best practices, including best practices coming from the standards community, including NERC, NIST, and ISA. In detection and recovery, we propose leveraging techniques such as anomaly detection to identify certain types of attacks and employing model-based schemes that present the security problem as a game between the attacker and defender as well as improving human-in-the-loop information awareness and taking advantage of automatic recovery characteristics of autonomous, real-time decision making algorithms inherent in many control systems and cyber-physical systems. In the area of resilience, established techniques such as redundancy, diversity, and the principle of least-privilege, and the separation of privilege apply. Such security principles, though, should be combined with novel control and estimation algorithms that address various types of attacks described previously to ensure systems are robust against a larger spectrum of attacks.

4.2 Very Large-Scale Information Assurance and Security Policy Management

We have developed concrete examples of targeted and denial of service attacks against spam filtering systems and used these attacks to understand the flaws in how machine learning has been applied. Based on the results, we developed highly effective countermeasures to the attacks. Similarly, we also developed long-duration attacks against the network flow anomaly detection system and used the results to design a new, robust network flow anomaly detection system. Also based on these research efforts, we launched a follow-on research effort that has developed techniques for analyzing the robustness of

machine learning algorithms' models to reverse engineering. This research will enable developers to analyze and characterize the resistance of various algorithms to attack.

Additional work that focused on the dynamics of interacting adaptive learning algorithms produced the following theoretical results:

- In repeated congestion games whose players adjust their choice of congestible resources using multiplicative-weights update algorithms (or, more generally, aggregate monotone selection dynamics) the distribution of play converges, in polynomial time, to a subset of Nash equilibria defined by a game-theoretic criterion that we refer to as "weakly stable".

- For almost all congestion games (in the sense of Lebesgue measure on the set of cost functions) the set of weakly stable Nash equilibria coincides with the set of pure Nash equilibria. In fact, the existence of a non-pure weakly stable Nash equilibrium implies a non-trivial polynomial relation among the values of the cost functions in the congestion game.

- The price of anarchy of the outcomes selected by multiplicative-weights algorithms can be exponentially better than the price of anarchy of the outcomes selected by certain other no-regret learning algorithms. This exponential separation exists even in the context of load-balancing games (i.e., when each algorithm is simply choosing one element from a set of congestible resources).

- The aforementioned exponential separation result for the price of anarchy in load-balancing games holds even in the more realistic "billboard model" (where agents can only see the actual measured congestion on each resource) assuming a bounded growth condition on the cost functions.

4.3 Scalable and Secure Discovery, Information Architecture, and Mediation

In the area of security protocols, there has been recent work on bridging the gap between competing approaches, with the goal of constructing a logic that can allow reasoning about quantitative aspects of security protocols, while still being amenable to mechanization. We showed how a logic that has already been widely used for nonmonotonic reasoning in Artificial Intelligence (AI) can do just that. The logic has "implications" of the form "$p \rightarrow q$"; roughly speaking, this says "the probability of q given p is high"; more precisely, "the probability of q given p approaches 1 super-polynomially, faster than any inverse polynomial". Thus, a statement like "secret encrypted $\rightarrow$ adversary does not decrypt" says "with high probability, if the secret is encrypted, the adversary does not decrypt it". We provided a sound and complete axiomatization for a large fragment of the logic and showed that, for this fragment, a qualitative proof of the correctness of a security protocol can be automatically converted to a quantitative proof appropriate for reasoning about concrete security. That is, if a conclusion can be proved qualitatively, then, given epsilon, we can find a delta such that the conclusion will hold with probability at least 1-epsilon if all the assumptions hold with probability at least 1-delta. Ongoing work is aimed at showing that this logic can be used to provide elegant correctness proofs for security protocols of interest.

Finally, in work that focused on building secure applications, there were a number of major research accomplishments. In the area of web applications, we advanced a "secure by construction" approach by developing tools that allow developers to leverage a security-typed language and compiler and developed Swift, a web application partitioning system. In the area of secure voting systems, we constructed Civitas, a secure internet voting system. In the area of building and integrating federated systems, we began developing the Fabric system, an infrastructure for securing federated systems that takes advantage

of distributed system resources while providing strong guarantees for information security and consistency.

5 PROGRAM PERSONNEL SUPPORTED

Below is a list of the personnel supported by the AF-TRUST project. Personnel are grouped by category and, within each category, listed alphabetically by last name.

- **Faculty**
  - Ken Birman (Cornell)
  - Ras Bodik (UC Berkeley)
  - Joe Halpern (Cornell)
  - Anthony Joseph (UC Berkeley)
  - Robert Kleinberg (Cornell)
  - Christoph Koch (Cornell)
  - Dexter Kozen (Cornell)
  - Edward Lee (UC Berkeley)
  - Andrew Myers (Cornell)
  - Rafael Pass (Cornell)
  - Radu Rugina (Cornell)
  - Shankar Sastry (UC Berkeley)
  - Doug Schmidt (Vanderbilt)
  - Emin Gün Sirer (Cornell)
  - Janos Sztipanovits (Vanderbilt)
  - Doug Tygar (UC Berkeley)
  - Robbert van Renesse (Cornell)

- **Post-Doctoral Scholars**
  - Alvaro Cárdenas (UC Berkeley)
  - Annarita Giani (UC Berkeley)
  - Qi Huang (Cornell)
  - Slobodan Matic (UC Berkeley)
  - Einar Vollset (Cornell)
  - Hakim Weatherspoon (Cornell)

- **Graduate Students**
  - Kamal Aboul-Hosn (Cornell)
  - Jong Hoon Ahnn (Cornell)
  - Gilad Arnold (UC Berkeley)
  - Manesh Balakrishnan (Cornell)
  - Marco Barreno (UC Berkeley)
  - Dmitri Chmelev (Cornell)
  - Stephen Chong (Cornell)
  - Michael Clarkson (Cornell)
  - Gan Deng (Vanderbilt)
  - Jeffrey Green (Vanderbilt)
  - Maya Haridasan (Cornell)
  - Jeffrey Hartline (Cornell)
  - Chi Ho (Cornell)
  - Ling Huang (UC Berkeley)
  - Chris Karlof (UC Berkeley)
  - Fang Liu (Cornell)
  - Isaac Liu (UC Berkeley)

- David Mandelin (UC Berkeley)
- Blaine Nelson (UC Berkeley)
- Krzysztof Ostrowski (Cornell)
- Deepak Parasam (Cornell)
- Lonnie Princehouse (Cornell)
- Benjamin Rubinstein (UC Berkeley)
- Nishanth Shankaran (Vanderbilt)
- Carlos Sakoda (Cornell)
- Alexa Sharp (Cornell)
- Yee Jiun Song (Cornell)
- Ymir Vigfusson (Cornell)
- Ming Xiong (Vanderbilt)
- Yang Zhao (UC Berkeley)
- Lantian Zheng (Cornell)
- Li Zhuang (UC Berkeley)

- **Undergraduate Students**
  - Chris Cai (UC Berkeley)
  - Steven Lee (UC Berkeley)

- **Staff**
  - Sally Alcala (UC Berkeley)
  - Christopher Brooks (UC Berkeley)
  - Larry Rohrbough (UC Berkeley)

Of the graduate students listed above, the following completed Masters or Doctoral degrees. For each student, their degree type and date awarded are listed as well as the title and a link to their thesis or dissertation if it is available online. Students are listed alphabetically by last name.

- Kamal Aboul-Hosn, *A Proof-Theoretic Approach to Mathematical Knowledge Management*, PhD, January 2007
- Mahesh Balakrishnan, *Reliable Communication for Datacenters*, PhD, January 2009
- Marco Barreno, *Evaluating the Security of Machine Learning Algorithms*, PhD, May 2008
- Stephen Chong, *Expressive and Enforceable Information Security Policies*, PhD, August 2008
- Michael Clarkson, *Quantification and Formalization of Security*, PhD, August 2009
- Gan Deng, *Deployment and Configuration of Component-Based Distributed, Real-Time and Embedded Systems*, PhD, December 2007
- Jeffrey Green, MS, 2009
- Maya Haridasan, *Techniques for Increasing Reliability and Scalability of Live Streaming Systems*, PhD, June 2008
- Jeffrey Hartline, *Incremental Optimization*, PhD, January 2008

- Ling Huang, *D-Trigger: A General Framework for Efficient Online Detection*, PhD, October 2007
- Chris Karlof, Human Factors in Web Authentication, PhD, February 2009
- Krzysztof Ostrowski, *Live Distributed Objects*, PhD, June 2008
- Benjamin Rubinstein (UC Berkeley), *Secure Learning and Learning for Security: Research in the Intersection*, PhD, May 2010
- Nishanth Shankaran, *Adaptive Resource Management Algorithms, Architectures, and Frameworks for Distributed Real-Time Embedded Systems*, PhD, December 2008
- Ming Xiong, MS, 2007
- Yang Zhao, *On the Design of Concurrent, Distributed Real-Time Systems*, PhD, August 2009
- Lantian Zheng, *Making Distributed Computing Secure by Construction*, PhD, January 2007
- Li Zhuang, *Security Inference from Noisy Data*, PhD, April 2008

6 PROGRAM-RELATED PUBLICATIONS

Below is a list of publications related to AF-TRUST research and development activities. Publications are listed in chronological order and are grouped by calendar year. For each publication, a hyperlink to an electronic version of the paper is also provided if the paper is available online.

2006

- Modularizing Variability and Scalability Concerns in Distributed Real-time and Embedded Systems with Modeling Tools and Component Middleware. Gan Deng, Douglas C. Schmidt, Anirudda Gokhale, and Andrey Nechypurenko. In Proceedings of the 9th IEEE International Symposium on Object-oriented Real-time Distributed Computing (ISORC '06), April 24-26, 2006, Gyeongju, Korea.

- How the Hidden Hand Shapes the Market for Software Reliability. Ken Birman, Coimbatore Chandersekaran, Danny Dolev, and Robbert van Renesse. In Proceedings of the First IEEE Workshop on Applied Software Reliability, Philadelphia, PA. June 2006.

- Reliable Multicast for Time-Critical Systems. Mahesh Balakrishnan and Ken Birman. In Proceedings of the First IEEE Workshop on Applied Software Reliability (WASR 2006), Philadelphia, PA. June 2006.

- Network-Aware Adaptation Techniques for Mobile File Systems. Benjamin Atkin, Ken Birman. In Proceedings of the 5th IEEE International Symposium on Network Computing and Applications (IEEE NCA06). Cambridge, MA. June 2006.

- Decentralized Robustness. Stephen Chong, Andrew C. Myers. In Proceedings of the 19th IEEE Computer Security Foundations Workshop, 242-253, July, 2006.

- Hierarchical Control of Multiple Resources in Distributed Real-time and Embedded Systems. Nishanth Shankaran, Xenofon Koutsoukos, Chenyang Lu, Douglas C. Schmidt, and Yuan Xue. In Proceedings of the 18th Euromicro Conference on Real-Time Systems (ECRTS 06), Dresden, Germany, July 5-7, 2006.

- Memory Leak Analysis by Contradiction. M. Orlovich and R. Rugina. In Proceedings of International Static Analysis Symposium (SAS '06), Seoul, Korea, August 2006.

- Defense Against Intrusion in a Live Streaming Multicast System. Maya Haridasan, Robbert van Renesse. In Proceedings of the 6th IEEE International Conference on Peer-to-Peer Computing (P2P2006), Cambridge, UK, September 2006.

- Scalable Services Architecture. Tudor Marian, Ken Birman, and Robbert van Renesse. In Proceedings of the IEEE Symposium on Reliable Distributed Systems (SRDS 2006). Leeds, UK. October 2006.

- Application of Programming Temporally Integrated Distributed Embedded Systems. Yang Zhao, Edward A. Lee and Jie Liu. In Proceedings of 2006 IEEE 1588 Conference Gaithersburg, MD, October 2-4, 2006.

- Joint Modeling and Design of Wireless Networks and Sensor Node Software. Elaine Cheong, Edward A. Lee and Yang Zhao. EECS Department, University of California, Berkeley, UCB/EECS-2006-150, November 17, 2006.

- The QuickSilver Properties Framework. Krzysztof Ostrowski, Ken Birman, Danny Dolev. Abstract, presented at the OSDI'06 poster session, Seattle, WA, November 2006.

- Securing Bgp Using External Security Monitors. Patrick Reynolds, Oliver Kennedy, Emin Gun Sirer, and Fred B. Schneider. Cornell University, Computing and Information Science, Technical Report TR2006-2065, Ithaca, New York, December 2006.

- Reinventing Computing for Real Time. Edward A. Lee and Yang Zhao. In Proceedings of the Monterey Workshop 2006, LNCS 4322, pp. 1-25, 2007, F. Kordon and J. Sztipanovits (Eds.) © Springer-Verlag Berlin Heidelberg 2007. The 2006 Technical Report that preceded this publication.

- Memory Leak Analysis by Contradiction. M. Orlovich and R. Rugina. Technical Report. 2006.

2007

- The Design and Application of Structured Types in Ptolemy II. Y. Zhao, Y. Xiong, E.A. Lee, X. Liu, L.C. Zhong. EECS Department, University of California, Berkeley, UCB/EECS-2007-21, January 30, 2007.

- Latency- And Bandwidth-minimizing Optimal Failure Detectors. Kelvin So and Emin Gün Sirer. In Proceedings of the European Conference on Computer Systems, Lisbon, Portugal, March 2007.

- Declarative Reliable Multi-Party Protocols Krzysztof Ostrowski, Ken Birman, Danny Dolev. Cornell University Technical Report (TR2007-2088). April, 2007.

- Implementing High-Performance Multicast in a Managed Environment. Krzysztof Ostrowski, Ken Birman, Danny Dolev. Cornell University Technical Report (TR2007-2087). April, 2007.

- Octant: A Comprehensive Framework For The Geolocalization Of Internet Hosts. Bernard Wong, Ivan Stoyanov, and Emin Gün Sirer. In Proceedings of the Symposium on Networked System Design and Implementation, Cambridge, Massachusetts, April 2007.

- Evaluating Technologies for Tactical Information Management in Net-Centric Systems. Ming Xiong, Jeff Parsons, James Edmondson, Hieu Nguyen, and Douglas C. Schmidt. In Proceedings of the Defense Transformation and Net-Centric Systems conference, April 9-13, 2007, Orlando, Florida.

- A Programming Model for Time-Synchronized Distributed Real-Time Systems. Yang Zhao, Jie Liu and Edward A. Lee. In Proceedings of the 13th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 07), Bellevue, WA, United States, April 3-6, 2007.

- FirePatch: Secure and Time-Critical Dissemination of Software Patches. Håvard Johansen, Dag Johansen, and Robbert van Renesse. In Proceedings of the IFIP International Information Security Conference (IFIPSEC 2007), Sandton, South-Africa, May 2007.

- The Design and Performance of Configurable Component Middleware for End-to-End Adaptation of Distributed Real-time Embedded Systems. Nishanth Shankaran, Douglas C. Schmidt, Yingming Chen, Xenofon Koutsoukous, and Chenyang Lu. In Proceedings of the 10th IEEE International Symposium on Object/Component/Service-oriented Real-time Distributed Computing, May 7-9, 2007, Santorini Island, Greece.

- Exploiting Gossip for Self-Management in Scalable Event Notification Systems. Ken Birman, Anne-Marie Kermarrec, Krzysztof Ostrowski, Marin Bertier, Danny Dolev, and Robbert Van Renesse. Distributed Event Processing Systems and Architecture Workshop (DEPSA), June 2007.

- Practical Memory Leak Detection using Guarded Value Flow Analysis. S. Cherem, L. Princehouse, and R. Rugina. In Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI '07), San Diego, CA, June 2007.

- SIF: Enforcing Confidentiality and Integrity in Web Applications. Stephen Chong, K. Vikram, Andrew C. Myers. In Proceedings of the 16th USENIX Security Symposium, pages 1–16, August 2007.

- Database Research Opportunities in Computer Games. Walker White, Christoph Koch, Nitin Gupta, Johannes Gehrke, and Alan Demers. SIGMOD Record, September 2007

- Secure Web Applications via Automatic Partitioning. Stephen Chong, Jed Liu, Andrew C. Myers, Xin Qi, K. Vikram, Lantian Zheng, Xin Zheng. In Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP'07), pages 31–44, October 2007. (Best paper award)

- Sliver: A Fast Distributed Slicing Algorithm. Vincent Gramoli, Ymir Vigfusson, Ken Birman, Anne-Marie Kermarrec, Robbert van Renesse. Technical Report. December 2007.

- Making Distributed Systems Robust. Chi Ho, Danny Dolev, and Robbert van Renesse. In Proceedings of the 11th International Conference On Principles Of Distributed Systems (OPODIS'07), Guadeloupe, West Indies, December 2007.

- Self-Stabilizing and Byzantine-Tolerant Overlay Network. Ezra Hoch, Danny Dolev, and Robbert van Renesse. In Proceedings of the 11th International Conference On Principles Of Distributed Systems (OPODIS'07), Vol. LNCS 4878, Springer, Guadeloupe, West Indies, December 2007.

- Massively Multi-Query Join Processing in Publish/Subscribe Systems. Alan Demers, Johannes Gehrke, Mingsheng Hong, Christoph Koch, Mirek Riedewald, and Walker White. In Proceedings of SIGMOD 2007

2008

- Enforcing Fairness in a Live-Streaming System. Maya Haridasan, Ingrid Jansch-Porto, Kenneth Birman, and Robbert van Renesse. In Proceedings of Multimedia Computing and Networking (MMCN 08), January 2008.

- The Building Blocks of Consensus. Yee Jiun Song, Robbert van Renesse, Fred B. Schneider, Danny Dolev. In Proceedings of the 9th International Conference on Distributed Computing and Networking (ICDCN '08), Kolkata, India. January, 2008.

- Gossip-based Distribution Estimation in Peer-to-Peer Networks. Maya Haridasan, Robbert van Renesse. In Proceedings of the 7th International Workshop on Peer-to-Peer Systems (IPTPS '08). Tampa Bay, FL. February 25-26, 2008.

- Maelstrom: Transparent Error Correction for Lambda Networks. Mahesh Balakrishnan, Tudor Marian, Ken Birman, Hakim Weatherspoon, Einar Vollset. USENIX Symposium on Networked System Design and Implementation (NSDI 08). April 2008.

- Brief Announcement: A Fast Distributed Slicing Algorithm. Vincent Gramoli, Ymir Vigfusson, Ken Birman, Anne-Marie Kermarrec, and Robbert van Renesse. In Proceedings of the 27th Annual Symposium on Principles of Distributed Computing (PODC'08), April 2008.

- Nysiad: Practical Protocol Transformation to Tolerate Byzantine Failures. Chi Ho, Robbert van Renesse, Mark Bickford, and Danny Dolev. USENIX Symposium on Networked System Design and Implementation (NSDI 08). San Francisco, CA. April 2008.

- Exploiting machine learning to subvert your spam filter. Blaine Nelson, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin I. P. Rubinstein, Udam Saini, Charles Sutton, J. D. Tygar, and Kai Xia. In Proceedings of the First Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), April 2008.

- Towards an Integrated Planning and Adaptive Resource Management Architecture for Distributed Real-time Embedded Systems. Nishanth Shankaran, John S. Kinnebrew, Xenofon D. Koutsoukos, Chenyang Lu, Douglas C. Schmidt, and Gautam Biswas. In Proceedings of the Workshop on Adaptive and Reconfigurable Embedded Systems (APRES) at the 14th IEEE Real-Time and Embedded Technology and Applications Symposium, St. Louis, MO, United States, April 22 - April 24, 2008.

- Evaluating the security of machine learning algorithms. (PhD dissertation). Marco Antonio Barreno. UC Berkeley, Department of EECS technical report UCB/EECS-2008-63, May 20 2008.

- Civitas: Toward a Secure Voting System. Michael R. Clarkson, Stephen Chong, Andrew C. Myers. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (Oakland), pages 354–368, May 2008.

- CaDANCE: A Criticality-Aware Deployment And Configuration Engine. Gan Deng, Douglas C. Schmidt, and Aniruddha Gokhale. In Proceedings of the 11th IEEE International Symposium on Object/Component/Service-oriented Real-time Distributed Computing, Orlando, Florida, May 5-7, 2008.

- PTIDES: A Programming Model for Distributed Real-Time Embedded Systems. P. Derler, T. H. Feng, E. A. Lee, S. Matic, H. D. Patel, Y. Zhao, and J. Zou. EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2008-72, May 2008.

- Compromising PCA-based anomaly detectors for network-wide traffic. Benjamin I. P. Rubinstein, Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Nina Taft, and Doug Tygar. UC Berkeley, Department of EECS technical report UCB/EECS-2008-73, May 29 2008.

- Machine Learning in the Presence of an Adversary: Attacking and Defending the SpamBayes Spam Filter. (Masters thesis). Udam Saini. UC Berkeley, Department of EECS technical report UCB/EECS-2008-62, May 20 2008.

- Approximate Matching For Peer-to-peer Overlays With Cubit. Bernard Wong, Aleksandrs Slivkins, and Emin Gün Sirer. Cornell University, Computing and Information Science, Ithaca, New York, May 2008.

- Tempest: Soft State Replication in the Service Tier. Tudor Marian, Mahesh Balakrishnan, Ken Birman, Robbert van Renesse. In Proceedings of the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-DCCS 2008), June 2008, Anchorage, AL.

- Cyber Security: Basic Defenses and Attack Trends. Alvaro A. Cárdenas, Tanya Roosta, Gelareh Taban, Shankar Sastry. In Giorgio Franceschetti and Marina Grossi Eds. Homeland Security Technology Challenges: From Sensing and Encrypting to Mining and Modeling. Artech House Publishers. 685 Canon Street; Norwood MA 02062. July 31, 2008. (Book Chapter)

- Secure Control: Towards Survivable Cyber-Physical Systems. Alvaro A. Cárdenas, Saurabh Amin, Shankar Sastry. In Proceedings of the First International Workshop on Cyber-Physical Systems (WCPS2008). Beijing, China, June 2008.

- Research Challenges for the Security of Control Systems. Alvaro A. Cárdenas, Saurabh Amin, Shankar Sastry. In Proceedings of the 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium, San Jose, CA, July 2008.

- Programming with Live Distributed Objects. Krzysztof Ostrowski, Ken Birman, Danny Dolev, and Jong Hoon Ahnn. In Proceedings of the 22nd European Conference on Object-Oriented Programming (ECOOP 2008). Cyprus. July 2008. J. Vitek, Ed. Lecture Notes In Computer Science, vol. 5142. Springer-Verlag, Berlin, Heidelberg, 463-489.

- QuickSilver Scalable Multicast (QSM). Krzysztof Ostrowski, Ken Birman, Danny Dolev. In Proceedings of the 7th IEEE International Symposium on Network Computing and Applications (IEEE NCA 2008). Cambridge, MA. July 2008.

- Sliver: A Fast Distributed Slicing Algorithm (Brief Announcement). Vincent Gramoli, Ymir Vigfusson, Ken Birman, Anne-Marie Kermarrec, Robbert van Renesse. In Proceedings of the Principles of Distributed Computing (PODC). Toronto, Canada. August 2008.

- Hierarchical Control of Multiple Resources in Distributed Real-time and Embedded Systems. Nishanth Shankaran, Xenofon Koutsoukos, Chenyang Lu, Douglas C. Schmidt, and Yuan Xue. The Springer Real-time Systems Journal, Volume 39, Numbers 1-3, August, 2008, pgs. 237-282.

- Bosco: One-Step Byzantine Aysnchronous Consensus. Yee Jiun Song, Robbert van Renesse. In Proceedings of the 22nd International Symposium on Distributed Computing (DISC 2008). Arcachon, France, September, 2008.

- Using Live Distributed Objects for Office Automation. Jong Hoon Ahnn, Ken Birman, Krzysztof Ostrowski, and Robbert van Renesse. In Proceedings of the ACM/IFIP/USENIX 9th International Middleware Conference, September 2008.

- Simulation and Implementation of the PTIDES Programming Model. Patricia Derler, Edward A. Lee, Slobodan Matic. In Proceedings of the 12th IEEE International Symposium on Distributed Simulation and Real Time Applications (DS-RT), pp. 330-333, IEEE Computer Society, October, 2008.

- Predictable Programming on a Precision Timed Architecture. Ben Lickly, Isaac Liu, Sungjun Kim, Hiren D. Patel, Stephen A. Edwards and Edward A. Lee. In Proceedings of International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES), Piscataway, NJ, pp. 137-146, IEEE Press, October, 2008.

- Dr. Multicast: Rx for Datacenter Communication Scalability. Ymir Vigfusson, Hussam Abu-Libdeh, Mahesh Balakrishnan, Ken Birman, Yoav Tock. In Proceedings of HotNets VII: Seventh ACM Workshop on Hot Topics in Networks. October 6-7, 2008. Calgary, Canada.

- Using Live Distributed Objects for Office Automation. Jong Hoon Ahnn, Ken Birman, Krzysztof Ostrowski, Robbert van Renesse. In Proceedings of the ACM/IFIP/USENIX 9th International Middleware Conference. Leuven, Belgium. December 2008.

- Device Driver Safety Through A Reference Validation Mechanism. Dan Williams, Patrick Reynolds, Kevin Walsh, Emin Gün Sirer, and Fred B. Schneider. In Proceedings of the Symposium on Operating System Design and Implementation, San Diego, California, December 2008.

- Open Problems in the Security of Learning. Marco Barreno, Peter L. Bartlett, Fuching Jack Chi, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, Udam Saini, and J. D. Tygar. In the Proceedings of the First ACM Workshop on Security and Artificial Intelligence (AISec), pg. 19-26, 2008.

- From qualitative to quantitative proofs of security properties using first-order conditional logic. J. Y. Halpern. In Proceedings of the Twenty-Third AAAI Conference on Artificial Intelligence (AAAI-08, 2008, pp. 454--459.

- Enforcing Fairness in a Live-Streaming System. Maya Haridasan, Ingrid Jansch-Porto, Robbert van Renesse. In Proceedings of Multimedia Computing and Networking (MMCN 2008), San Jose, CA.

- Adaptive One-way Functions and Applications. O. Pandey, R. Pass and V. Vaikuntanathan. In Proceedings of Crypto'08.

- Evading Anomaly Detection through Variance Injection Attacks on PCA (Extended Abstract). Benjamin I. P. Rubinstein, Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Nina

Taft, and J. D. Tygar. In Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection (RAID), pg. 394-395, 2008. Winner of the RAID08 Best Poster Award.

- Design and Performance Evaluation of an Adaptive Resource Management Framework for Distributed Real-time and Embedded Systems. Nishanth Shankaran, Douglas C. Schmidt, Xenofon D. Koutsoukos, Yingming Chen, and Chenyang Lu. EURASIP Journal on Embedded Systems (EURASIP JES): Special issue on Operating System Support for Embedded Real-Time Applications, Edited by Alfons Crespo, Ismael Ripoll, Michael Gonzalez Harbour, and Giuseppe Lipari, 2008, pgs. 47-66.

2009

- The Monoculture Risk Put into Context. Fred Schneider and Ken Birman. In IEEE Security & Privacy, Vol. 7, Number 1. Pages 14-17. January/February 2009.

- Poster Abstract: Timing Instruction – ISA Extensions for Timing Guarantees. Isaac Liu, Ben Lickly, Hiren D. Patel, Edward A. Lee. In Proceedings of the 15th IEEE Real-Time and Embedded Technology and Applications Symposium, April, 2009.

- Poster Abstract: PtidyOS: An Operating System based on the PTIDES Programming Model. Shanna-Shaye Forbes, Jia Zou, Slobodan Matic, Edward A. Lee. In Proceedings of the 15th IEEE Real-Time and Embedded Technology and Applications Symposium, April, 2009.

- Execution Strategies for PTIDES, a Programming Model for Distributed Embedded Systems. J. Zou, S. Matic, E. A. Lee, T. H. Feng, P. Derler. In Proceedings of the 15th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), IEEE Press, pp. 77-86, April, 2009.

- Learning prediction suffix trees with Winnow. Nikos Karampatziakis and Dexter Kozen. In Léon Bottou and Michael Littman, editors. In Proceedings of the 26th International Conference on Machine Learning (ICML'09), pages 489-496, Montreal, Canada, June 2009. Omnipress.

- Multiplicative updates outperform generic no-regret learning in congestion games: extended abstract. R. Kleinberg, G. Piliouras, and E. Tardos. In Proceedings of the 41st Annual ACM Symposium on theory of Computing (Bethesda, MD, USA, May 31 - June 2, 2009). STOC '09. ACM, New York, NY, 533-542.

- The Case for Timing-Centric Distributed Software. Edward A. Lee, Slobodan Matic, Sanjit A. Seshia, Jia Zou. In Proceedings of the IEEE International Conference on Distributed Computing Systems Workshops: Workshop on Cyber-Physical Systems, IEEE, pp. 57-64, June, 2009.

- Challenges for the Security of Cyber Physical Systems. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry. In DHS Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, July 2009.

- Distributed Slicing. Vincent Gramoli, Ymir Vigfusson, Ken Birman, Anne-Marie Kermarrec, and Robbert van Renesse. IEEE Transactions on Computers, Special Issue on Autonomic Network Computing. Idit Keidar (ed.), Vol. 58. No. 11, IEEE Computer Society Press, July 2009.

- Load Balancing Without Regret in the Bulletin Board Model. Kleinberg, G. Piliouras, and E. Tardos. In Proceedings of the 28th ACM Symposium on Principles of Distributed Computing (Calgary, AB, Canada, August 10 - 12, 2009). PODC '09. ACM, New York, NY, 56-62.

- Fabric: A Platform for Secure Distributed Computation and Storage. Jed Liu, Michael D. George, K. Vikram, Xin Qi, Lucas Waye, and Andrew C. Myers. In Proceedings of the ACM 2009 Symposium on Operating Systems Principles and Implementation (SOSP 2009), pages 321–334, October 11–14, 2009.

- An Integrated Planning and Adaptive Resource Management Architecture for Distributed Real-time Embedded Systems. Nishanth Shankaran, John Kinnebrew, Xenofon Koutsoukos, Chenyang Lu, Douglas C. Schmidt, and Gautam Biswas. IEEE Transactions on Computers, Special Issue on Autonomic Network Computing, volume 58, number 11, 1485-1498, November 2009.

- Database Research in Computer Games. Alan Demers, Johannes Gehrke, Christoph Koch, Ben Sowell, and Walker White. SIGMOD 2009. Tutorial.

- Quantifying Information Flow with Beliefs. Michael R. Clarkson, Andrew C. Myers, Fred B. Schneider. Journal of Computer Security, 17(5):655–701, 2009.

- A Compositional Framework for Complex Queries over Uncertain Data. Michaela Goetz and Christoph Koch. In Proceedings of ICDT 2009.

- A Logical Characterization of Iterated Admissibility. J. Halpern and R. Pass. In Proceedings of TARK'09.

- Iterated Regret Minimization: A New Solution Concept. J. Halpern and R. Pass. In Proceedings of IJCAI'09.

- An Epistemic Characterization of Zero Knowledge. J. Halpern, R. Pass and V. Raman. In Proceedings of TARK'09.

- Rule-Based Multi-Query Optimization. Mingsheng Hong, Mirek Riedewald, Christoph Koch, Johannes Gehrke, and Alan Demers. In Proceedings of EDBT 2009.

- A Unified Framework for Concurrent Security: Universal Composability from Stand-alone Non-malleability. H. Lin, R. Pass and M. Venkitasubramaniam. In Proceedings of STOC'09.

- Non-malleability Amplification. H. Lin and R. Pass. In Proceedings of STOC'09.

- Misleading learners: Co-opting your spam filter. Blaine Nelson, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin I. P. Rubinstein, Udam Saini, Charles Sutton, J. D. Tygar, and Kai Xia. Book chapter in Jeffrey J. P. Tsai and Philip S. Yu (eds.) Machine Learning in Cyber Trust: Security, Privacy, and Reliability, pg. 17-51, 2009.

- ANTIDOTE: Understanding and Defending against Poisoning of Anomaly Detectors. Benjamin I. P. Rubinstein, Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao,

Nina Taft, and J. D. Tygar. In the Proceedings of the Ninth Internet Measurement Conference (IMC), pg. 1-14, 2009.

2010

- A Middleware for Gossip Protocols. Michael Chow and Robbert van Renesse. International Workshop on Peer-to-Peer Systems (IPTPS 2010), San Jose, CA. April 2010.

- Secure Learning and Learning for Security: Research in the Intersection. (PhD dissertation). Benjamin Rubinstein. UC Berkeley, Department of EECS technical report UCB/EECS-2010-71, May 13 2010.

- Near-Optimal Evasion of Convex-Inducing Classifiers. Blaine Nelson, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Steven Lee, Satish Rao, Anthony Tran and J. D. Tygar. In the Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics (AISTATS), pg. 549-556, 2010.

- The Security of Machine Learning. Marco Barreno, Blaine Nelson, Anthony D. Joseph, and J. D. Tygar. To appear in Machine Learning.

- Stealthy Poisoning Attacks on PCA-based Anomaly Detectors. Benjamin I. P. Rubinstein, Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft, and J. D. Tygar. To appear in ACM SIGMETRICS Performance Evaluation Review, 2010.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
26-07-2010	Final	Apr 2006 - Feb 2009

4. TITLE AND SUBTITLE
AF-TRUST, Air Force Team for Research in Ubiquitous Secure Technology
Final Performance Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-06-1-0244

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Birman, Kenneth P.
Rohrbough, Laurence J.
Sastry, S. Shankar
Schmidt, Douglas C.
Sztipanovits, Janos

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Cornell University, Ithaca, NY
University of California, Berkeley, CA
Vanderbilt University, Nashville, TN

8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Office of Scientific Research
875 N. Randolph St., Room 3112
Arlington, VA 22203

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Scientific Research
875 N. Randolph St., Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-OSR-VA-TR-2012-0675

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unlimited distribution.

13. SUPPLEMENTARY NOTES
None.

14. ABSTRACT
AF-TRUST was established to address Air Force challenges associated with the Global Information Grid (GIG) and Network Centric Enterprise Systems (NCES). The AF-TRUST team (Berkeley, Cornell, Vanderbilt) focused on top Air Force research priorities and advanced the state-of-the-art in cyber-assurance to address key trust- and Quality of Service (QoS)-related properties simultaneously throughout the lifecycles of large-scale Air Force systems. This was done via a novel combination of analytical and experimental techniques with research and development activities focused in three areas: (1) Scalable, Real-Time, and Fault-Tolerant Quality of Service (QoS), (2) Very Large-Scale Information Assurance and Security Policy Management, and (3) Scalable and Secure Discovery, Information Architecture, and Mediation.

15. SUBJECT TERMS
Berkeley, Cornell, Command and Control, Cybersecurity, Global Information Grid (GIG), Information Assurance, Information Security, Network Centric Enterprise System (NCES), Quality of Service (QoS), Resilience, Security, TRUST, Vanderbilt

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Laurence J. Rohrbough
U	U	U	UU	1	19b. TELEPHONE NUMBER (Include area code) 510-643-3032